IN THE UNITED STATES DISTRICT COURT
DISTRICT OF NEBRASKA

LESLIE COOK, individually and on behalf of all others similarly situated, Plaintiff, v. REGIONAL CARE, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Leslie Cook, individually, and on behalf of all similarly situated persons, alleges the following against Defendant Regional Care, Inc. ("Defendant"), based on Plaintiff's own personal knowledge and on information and belief derived from, among other things, investigation by counsel and review of public documents, as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and other similarly situated individuals' ("Class Members," as defined *infra*) personally identifying information ("PII") and personal health information ("PHI").

2. Defendant is a third-party health plan administrator that provides services to more than 25,000 members in Nebraska and across the country.

3. On or about September 18, 2024, Defendant detected suspicious activity on its computer network. Defendant identified individuals whose personal information may be involved and determined that the data at issue includes "full name, dates of birth, Social Security number, medical information, and health insurance information." ("Data Breach").[1]

[1] *Regional Care, Inc. Notifies Customers and Clients of Data Security Incident* (Dec. 16, 2024),

4. Defendant began sending out notice letters to impacted persons, on or about December 16, 2024.

5. Based on Plaintiff's and Class Members' beliefs, Defendant is the entity with primary responsibility for this Data Breach.

6. Defendant notified approximately 225,728 individuals of the Data Breach.[2]

7. Defendant failed to adequately protect Plaintiff's and Class Members' PII/PHI—and failed to encrypt or redact this highly sensitive information. This unencrypted, unredacted PII/PHI was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect its customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII/PHI because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

8. Plaintiff brings this action on behalf of all persons whose PII/PHI was compromised as a result of Defendant's failure to: (i) adequately protect the PII/PHI of Plaintiff and Class Members; (ii) adequately vet its data security practices; (iii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iv) effectively secure hardware containing protected PII/PHI using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal law.

9. Defendant disregarded the rights of Plaintiff and Class Members by intentionally,

---

https://www.regionalcare.com/_files/ugd/08cced_e2e1b5bf773f46c5af66062f13ade51b.pdf (last visited Dec. 28, 2024).

[2] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b76b9e24-3713-4701-9fe4-cd0dfe396076.html (last visited Dec. 30, 2024).

willfully, recklessly, or negligently failing to ensure that Defendant had adequate and reasonable safeguards and measures in place to protect the PII/PHI of Plaintiff and Class Members after that information was transferred and entrusted to it in the regular course of business.

10. More specifically, Defendant failed to take and implement available steps to prevent an unauthorized disclosure of data, and failed to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption, storage, and destruction of data, even for internal use. As a result, the PII/PHI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third parties.

11. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe and they should be entitled to injunctive and other equitable relief.

12. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost or diminished value of PII/PHI; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their PII/PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's custody, control, or possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI.

13. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose PII/PHI was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

II. PARTIES

14. Plaintiff Leslie Cook is a citizen and resident of Nebraska. Plaintiff provided PII/PHI to Defendant or otherwise had their PII/PHI provided to Defendant. Plaintiff received a breach notice letter from Defendant confirming Plaintiff was impacted by the Data Breach.

15. Defendant Regional Care, Inc. is incorporated under the laws of Nebraska with a principal place of business located at 905 West 27th Street in Scottsbluff, Nebraska.

III. JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are Class Members who are diverse from Defendant, and (4) there are more than 100 Class Members.

17. The Court has general personal jurisdiction over Defendant because Defendant has its principal place of business in this District.

18. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendant resides in this District.

IV. FACTUAL ALLEGATIONS

A. Defendant's Business

19. Defendant offers health plan administration services to clients and brokers.[3]

20. In the regular course of their business, Defendant collects highly private PII/PHI from its customers and other individuals who interact or otherwise transact with Defendant for business purposes. Defendant stores this highly sensitive information digitally.

[3] *About Regional Care, Inc.*, Regional Care, Inc., https://www.regionalcare.com/about (last visited Dec. 30, 2024).

21. On information and belief, Plaintiff and Class Members provided personal information directly or indirectly to Defendant through Defendant's clients or brokers in exchange for health plan management services. Included in the sensitive information provided to Defendant, per Defendant's breach notice letter, is at least Plaintiff's and Class Members' names, dates of birth, Social Security numbers, and other medical and health insurance, but other information may also be provided.

22. Defendant was obligated, as a vendor that collects sensitive consumer data, to protect that information.

23. On information and belief, Defendant is required by law (including but not limited to HIPAA) to maintain the privacy and security of individuals' health and medical information and to provide individuals with notice if a breach occurs that may have compromised the privacy or security of that medical information.

24. Defendant also had a duty to adopt reasonable measures to protect the PII/PHI of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant had a legal duty to keep its customers' PII/PHI safe and confidential.

25. Defendant also had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA") and industry standards to keep PII/PHI confidential and to protect it from unauthorized access and disclosure.

26. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII/PHI. Without the required submission of PII/PHI, Defendant could not perform the services it provides and monetize its business.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII/PHI, Defendant assumed legal and equitable duties and knew or should have known

it was responsible for protecting Plaintiff's and Class Members' PII/PHI from disclosure.

B. The Data Breach

28. Defendant began sending notices of the data breach to impacted persons on or about December 16, 2024. It also placed a notice ("Notice") on its website.[4]

29. According to the Notice, on or about September 18, 2024, Defendant detected the Data Breach.[5] The Notice provides:

> After an extensive forensic investigation and manual document review, we concluded on or about November 8, 2024 that one or more of the files potentially accessed and/or acquired by the unauthorized party contained some sensitive personal information. The potentially impacted information varies by individual, and may include the impacted individual's full name, dates of birth, Social Security number, medical information, and health insurance information.
>
> Out of an abundance of caution, commencing on December 16, 2024, RCI notified individuals whose information may have been included in the files accessed by the unauthorized party. Notified individuals have been provided with best practices to protect their information, and individuals whose Social Security numbers were contained in the impacted files have been offered complimentary credit monitoring.[6]

30. Despite knowing about the breach as early as September 18, 2024, Defendant did not post the Notice and commence sending notice letters until approximately two months later, on December 16, 2024.

31. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, causing the exposure of PII/PHI. Nor did Defendant take the precautions and measures needed to ensure Defendant's data security protocols were sufficient to protect the PII/PHI in its custody, control, or possession.

---

[4] *Regional Care, Inc. Notifies Customers and Clients of Data Security Incident*, *supra* note 1.
[5] *Id.*
[6] *Id.*

32. As a result, the third-party accessed and acquired files containing unencrypted PII/PHI of Plaintiff and Class Members.

33. Defendant's failure to promptly notify Plaintiff and Class Members that their PII/PHI was accessed and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that PII/PHI before Plaintiff and Class Members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class Members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

C. Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII/PHI

34. Defendant derives a substantial economic benefit from providing services to its customers, and as a part of providing those services, Defendant retains and stores the PII/PHI of its customers and of other individuals who interact or otherwise transact with Defendant for business purposes, including that of Plaintiff and Class Members.

35. By obtaining, collecting, and storing the PII/PHI of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting the PII/PHI from disclosure.

36. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII/PHI.

37. Plaintiff and Class Members relied on Defendant to keep their PII/PHI confidential and maintained securely, to use this information for business purposes only, to provide the information only to trusted and secure vendors and other third parties, and to make only authorized disclosures of this information.

38. Defendant could have prevented this Data Breach by properly securing the PII/PHI

of Plaintiff and Class Members.

39. Defendant's negligence in safeguarding the PII/PHI of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

D. Defendant Knew or Should Have Known of the Risk Because Institutions in Possession of PII/PHI Are Particularly Susceptible to Cyberattacks

40. Defendant's data security obligations were particularly important given the ubiquity of cyberattacks and/or data breaches targeting institutions that collect and store PII/PHI, like Defendant, preceding the date of the Data Breach.

41. Data thieves regularly target companies that receive and maintain PII/PHI due to the highly sensitive nature of that information. Defendant knew and understood that unprotected PII/PHI is valuable and highly sought after by criminal parties who seek to illegally monetize that PII/PHI through unauthorized access.

42. In 2023, a record 3,205 publicly reported data breaches occurred, resulting in approximately 353,027,982 individuals being compromised, a 78% increase from a record high 2022.[7]

43. In view of the continuing spike in data breaches, Defendant knew or should have known the PII/PHI it collected and maintained would be targeted by cybercriminals.

44. Further, cybercriminals seek out private health information at a greater rate than other sources of personal information. In a 2024 report, the healthcare compliance company Protenus found that there were 1,161 medical data breaches in 2023 with over 171 million patient

[7] *ITRC 2023 Data Breach Report – Key Findings and Solutions*, Bluefin, https://www.bluefin.com/bluefin-news/itrc-2023-data-breach-report-key-findings-and-solutions/#:~:text=Over%209%25%20of%20the%203%2C700,compromise%20victims%20impacting%20210M%20victims (last visited Dec. 30, 2024).

records exposed.[8] This is an increase from the 1,138 medical data breaches which exposed approximately 59 million records that Protenus compiled in 2023.[9]

45. PII/PHI is a valuable property right.[10] The value of PII/PHI as a commodity is measurable.[11] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[12] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[13] PII and PHI are so valuable to identity thieves that once it has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

46. As a result of the real and significant value of these data, identity thieves and other cybercriminals have openly posted credit card numbers, Social Security numbers, PII/PHI, and other sensitive information directly on various internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data

---

[8] *2024 Breach Barometer*, Protenus - Industry Report, https://protenus.com/hubfs/Breach_Barometer/Latest%20Version/Protenus%20-%20Industry%20Report%20-%20Privacy%20-%20Breach%20Barometer%20-%202024.pdf (last visited Dec. 30, 2024).

[9] *Id*.

[10] Marc van Lieshout, *The Value of Personal Data*, ResearchGate (May 2015) https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data, ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible[.]").

[11] Robert Lowes, *Stolen EHR Charts Sell for $50 Each on Black Market*, Medscape (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[12] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLibrary (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[13] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, Interactive Advertising Bureau (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

47. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[14] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[15]

48. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[16] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[17]

49. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[18] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually

---

[14] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech Magazine (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").
[15] *Id.*
[16] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC Media (July 16, 2013), https://www.scworld.com/news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.
[17] *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain,* FBI Cyber Division (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[18] *What Happens to Stolen Healthcare Data?*, *supra* note 14.

transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[19]

50. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the figure is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[20]

51. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

52. As a custodian of PII/PHI, Defendant knew, or should have known, the importance of safeguarding the PII/PHI entrusted to it, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

53. Defendant was, or should have been, fully aware of the unique type and the significant volume of data it collected and maintained and, thus, the significant number of individuals who would be harmed by the exposure of that data.

54. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII/PHI of Plaintiff and Class Members from being compromised.

---

[19] *Id.*

[20] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*: *An Experimental Study*, Information Systems Research (June 2011), https://www.jstor.org/stable/23015560?seq=1.

55. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII/PHI of Plaintiff and Class Members, and Defendant's failure to adequately vet its vendors.

56. The ramifications of Defendant's failure to keep secure the PII/PHI of Plaintiff and Class Members are long-lasting and severe. Once PII/PHI is stolen—particularly Social Security numbers, which are confirmed to be impacted here—fraudulent use of that information and damage to victims may continue for years.

E. Value of Sensitive Personal Information

57. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[21] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[22]

58. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[23]

---

[21] 17 C.F.R. § 248.201 (2016).
[22] *Id.*
[23] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

59. For example, PII can be sold at a price ranging from $40 to $200.[24] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[25]

60. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, payment card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The type of highly sensitive information compromised in this Data Breach—Social Security numbers—is impossible to "close" and difficult, if not impossible, to change.

61. Indeed, due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[26]

62. Social Security numbers and other highly sensitive information (e.g., health information) demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[27]

---

[24] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[25] *In the Dark*, VPNOverview.com, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Dec. 28, 2024).
[26] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[27] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Network World (Feb. 6, 2015),

63. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing, or even give false information to police.

64. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[28]

F. Defendant Failed to Comply with FTC Guidelines

65. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

66. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating

---

https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[28] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extend Is Unknown*, U.S. Gov't Accountability Off. (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

67. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

68. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

69. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices, and those of its vendors. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

70. Defendant was at all times fully aware of its obligation to protect the PII/PHI it was entrusted with, yet failed to comply with such obligation. Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. Defendant Failed to Comply with Industry Standards

71. As noted above, experts studying cybersecurity routinely identify institutions like Defendant as being particularly vulnerable to cyberattacks because of the value of the PII/PHI

which it collects and maintains.

72. Some industry best practices that should be implemented by institutions dealing with sensitive PII/PHI, like Defendant, include, but are not limited to: educating all employees; strong password requirements; multilayer security, including firewalls; anti-virus and anti-malware software; encryption; multi-factor authentication; backing up data; and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all these industry best practices.

73. Other best cybersecurity practices that are standard at large institutions that store PII/PHI include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

74. Defendant failed to meet the minimum standards of, e.g., the NIST Cybersecurity Framework, and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established industry standards in reasonable cybersecurity readiness.

75. These foregoing frameworks are existing and applicable industry standards in the corporate sector and Defendant failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

76. Despite Defendant's obligations, Defendant failed to appropriately monitor and maintain its data security systems in a meaningful way so as to prevent the Data Breach.

77. Had Defendant properly maintained its systems and adequately protected them, it could have prevented the Data Breach.

H. Defendant Breached Its Duties to Safeguard Plaintiff's and Class Members' PII/PHI

78. In addition to its obligations under federal laws, Defendant owed duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed duties to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII/PHI of Class Members.

79. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of PII/PHI in a timely manner.

80. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

81. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of its inadequate data security practices.

82. Defendant breached its obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its data security practices. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' and other related individuals' PII/PHI;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

e. Failing to adhere to industry standards for cybersecurity as discussed above; and

f. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' PII/PHI.

83. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII/PHI by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted PII/PHI.

84. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII/PHI.

I. Common Injuries & Damages

85. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII/PHI ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of the value of their PII/PHI; (e) invasion of privacy; and (f) the continued risk to their PII/PHI, which remains in the possession of Defendant and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII/PHI.

J. The Data Breach Increases Victims' Risk of Identity Theft

86. Due to the Data Breach, Plaintiff and Class Members are at an indefinite, heightened risk of identity theft.

87. The unencrypted PII/PHI of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII/PHI may fall into the hands of companies that will use the detailed PII/PHI for targeted marketing without the approval of Plaintiff and Class Members.

88. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII/PHI to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft-related crimes discussed below.

89. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

90. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's log-in credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

91. One such example of criminals piecing together bits and pieces of compromised

PII for profit is the development of "Fullz" packages.[29]

92. With "Fullz" packages, cybercriminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

93. The development of "Fullz" packages means that the stolen PII/PHI from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, driver's license numbers, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

94. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[30]

---

[29] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, KrebsOnSecurity (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

[30] *2023 Consumer Impact Report*, Identity Theft Resource Center (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last visited Dec. 28, 2024).

95. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[31] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[32] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[33] The FTC also warns, "If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use."[34]

96. A report published by the World Privacy Forum and presented at the U.S. FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

a. Changes to their healthcare records, most often the addition of falsified information through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

b. Significant bills for medical goods and services neither sought nor received.

c. Issues with insurance, co-pays, and insurance caps.

---

[31] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, World Privacy Forum (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[32] *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 17.
[33] *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Advice (May 2021), https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Dec. 28, 2024).
[34] *Id*.

d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

g. Phantom medical debt collection based on medical billing or other identity information.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own. [35]

97. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[36]

98. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by someone intending to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

---

[35] *See The Geography of Medical Identity Theft*, *supra* note 31.

[36] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, Journal of Systemics, Cybernetics and Informatics (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

K. Loss of Time to Mitigate Risk of Identity Theft and Fraud

99. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII/PHI was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the resource and asset of time has been lost.

100. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

101. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[37]

102. These efforts are also consistent with the steps the FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[38]

---

[37] *See Data Breaches Are Frequent . . .*, *supra* note 28.
[38] *What To Do Right Away,* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited Dec. 28, 2024).

L. Diminution of Value of PII/PHI

103. PII/PHI is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyberthefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond a doubt that PII/PHI has considerable market value.

104. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[39]

105. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[40]

106. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[41]

107. Conversely, sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[42]

108. As a result of the Data Breach, Plaintiff's and Class Members' PII/PHI, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss.

---

[39] David Lazarus, *Shadowy data brokers make the most of their cloak,* Los Angeles Times (Nov. 5, 2019, 5 AM PT), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[40] Datacoup, Inc, https://datacoup.com/ (last visited Dec. 28, 2024).
[41] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Oct. 8, 2024).
[42] Ashiq JA, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

Moreover, the PII/PHI is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

M. Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

109. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII/PHI involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchased by criminals intending to utilize the PII/PHI for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims.

110. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

111. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

112. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost, for a minimum of five years, that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII/PHI.

N. Plaintiff Cook's Experience

113. Plaintiff provided PII/PHI, or had PII/PHI provided, to Defendant. Plaintiff trusted that vendors to whom Plaintiff's data would be provided would use reasonable measures to protect it according to internal policies and industry standards, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

114. At the time of the Data Breach, Defendant collected and retained Plaintiff's and Class Members' PII/PHI in its systems.

115. Plaintiff's and Class Members' PII/PHI was compromised in the Data Breach and stolen by cybercriminals.

116. Plaintiff has been injured by the compromise of Plaintiff's PII/PHI.

117. Plaintiff takes reasonable measures to protect PII/PHI. Plaintiff has never knowingly transmitted unencrypted PII/PHI over the internet or other unsecured source.

118. Plaintiff stores any documents containing PII/PHI in a safe and secure location and diligently chooses unique usernames and passwords for online accounts.

119. Had Plaintiff known that Defendant does not adequately protect PII/PHI, Plaintiff would not have agreed to provide sensitive PII/PHI to Defendant, or to allow Plaintiff's sensitive information to be provided to Defendant.

120. As a result of and following the Data Breach, Plaintiff has suffered a loss of time on issues related to this Data Breach to protect Plaintiff from identity theft and fraud. Plaintiff has monitored, and continues to monitor, accounts, credit reports and credit scores, and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties.

121. Plaintiff suffered interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy.

122. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from Plaintiff's PII/PHI being placed in the hands of criminals that will continue for Plaintiff's lifetime.

123. Defendant obtained and continues to maintain Plaintiff's PII/PHI, and thus has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure. Plaintiff's PII/PHI was compromised and disclosed as a result of the Data Breach.

124. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

125. Further, Plaintiff is and will remain at risk of harm in the future because Defendant continues to maintain Plaintiff's confidential PII/PHI but does not take adequate steps to protect that information from a data breach. Accordingly, Plaintiff's PII/PHI faces an imminent risk of disclosure in a future Defendant data breach.

V. CLASS ALLEGATIONS

126. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff seeks certification of the following classes (together, the "Class"):

> **Nationwide Class**
> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach, including all individuals who received notice of the Data Breach.
>
> **Nebraska Class**
> All individuals residing in Nebraska whose PII/PHI was compromised in the Data Breach, including all individuals who received notice of the Data Breach.

127. Excluded from the Class are Defendant and its parents or subsidiaries, any entities

in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned, as well as their judicial staff and immediate family members.

128. Plaintiff reserves the right to modify or amend the definition of the proposed Class, as well as to add subclasses, before the Court determines whether certification is appropriate.

129. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

130. **Numerosity**. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes the proposed Class includes nearly 226,000 individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant's records.

131. **Commonality**. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA;

c. When Defendant learned of the Data Breach;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII/PHI compromised in the Data Breach;

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

f. Whether Defendant's data security systems, prior to and during the Data Breach, were consistent with industry standards;

g. Whether Defendant owed duties to Class Members to safeguard their PII/PHI;

h. Whether Defendant breached its duties to Class Members to safeguard their PII/PHI;

i. Whether hackers obtained Class Members' PII/PHI via the Data Breach;

j. Whether Defendant had legal duties to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

k. Whether Defendant breached its duties to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

l. Whether Defendant knew or should have known its data security systems and monitoring processes were deficient;

m. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;

n. Whether Defendant's conduct was negligent;

o. Whether Defendant breached implied contracts with Plaintiff and Class Members;

p. Whether Defendant was unjustly enriched;

q. Whether Plaintiff and Class Members are entitled to damages;

r. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

s. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

132. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII/PHI, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through Defendant's common misconduct. Plaintiff is advancing the same claims and legal theories on behalf of Plaintiff and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

133. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

134. **Predominance**. Defendant has engaged in common courses of conduct toward Plaintiff and Class Members. For example, all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

135. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to

individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

136. Class certification is also appropriate under Federal Rule of Civil Procedure 23(b)(2). Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

137. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names, email and/or postal addresses, and phone numbers of Class Members affected by the Data Breach.

CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class or alternatively the Nebraska Class)

138. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

139. Defendant owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

140. Defendant knew the risks of collecting and storing Plaintiff's and all other Class Members' PII/PHI and the importance of maintaining secure systems. Defendant knew of the many data breaches that targeted healthcare providers in recent years.

141. Given the nature of Defendant's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities

to its systems and prevented the Data Breach from occurring.

142. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to them—including Plaintiff's and Class Members' PII/PHI.

143. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' PII/PHI to unauthorized individuals.

144. But for Defendant's negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their PII/PHI would not have been compromised.

145. As a result of Defendant's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant's

possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class or alternatively the Nebraska Class)

146. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

147. Defendant's duties arise from, *inter alia*, Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant, of failing to employ reasonable measures to protect and secure Private Information.

148. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class Members' Personal Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it obtains and stores, and the foreseeable consequences of a data breach involving Personal Information including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

149. Defendant's violations of Section 5 of the FTCA constitutes negligence per se.

150. Plaintiff and Class Members are within the class of persons that Section 5 of the FTCA were intended to protect.

151. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA was intended to guard against.

152. Defendant's duties also arise from the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected

Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

153. Defendant violated HIPAA Privacy and Security Rules by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII/PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

154. Defendant's violations of HIPAA constitutes negligence per se.

155. Plaintiff and Class Members are within the class of persons that HIPAA was intended to protect.

156. The harm occurring as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

157. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Personal Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' Personal Information to unauthorized individuals.

158. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendant's violations of law, including Section 5 of the FTCA and HIPAA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased

risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Personal Information; (iii) breach of the confidentiality of their Personal Information; (iv) deprivation of the value of their Personal Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class or alternatively the Nebraska Class)

167. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

168. This count is pleaded in the alternative to any contract or future contract claims.

169. Upon information and belief, Defendant funds their data security measures entirely from its general revenue, including from payments made by or on behalf of Plaintiff and Class Members, like Plaintiff, for services.

170. As such, a portion of the value and monies derived from payments made directly or indirectly by Class Members for services is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

171. Plaintiff and Class Members directly or indirectly conferred a monetary benefit on Defendant in providing it with their valuable PII/PHI.

172. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII/PHI of Plaintiff and Class Members for business purposes.

173. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' PII/PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures.

174. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profit over the requisite security.

175. Defendant failed to secure Plaintiff's and Class Members' PII/PHI and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII/PHI provided.

176. Under the principles of equity and good conscience, Defendant should not be permitted to retain the benefits that Plaintiff and Class Members conferred upon it.

177. Plaintiff and Class Members have no adequate remedy at law.

178. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII/PHI; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their PII/PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's custody, control, and possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI.

179. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other

compensation obtained by Defendant from its wrongful conduct.

180. This can be accomplished by establishing a constructive trust from which Plaintiff and Class Members may seek restitution or compensation.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiff and the Nationwide Class or alternatively the Nebraska Class)

181. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

182. Plaintiff and Class Members provided, directly or indirectly, Defendant their PII/PHI, believing that any vendor whose services were contracted for on behalf of them and that came into possession of this data would protect that information. Plaintiff and Class Members would not have provided or agreed to provide Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiff's and Class Members' PII/PHI created a fiduciary relationship between Defendant, on the one hand, and Plaintiff and Class Members, on the other hand. In light of this relationship, Defendant must act primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

183. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. Defendant breached that duty by failing to properly protect the integrity of its systems containing Plaintiff's and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by FTC and industry standards, and otherwise failing to safeguard Plaintiff's and Class Members' PII/PHI that it collected.

184. As a direct and proximate result of Defendant's breaches of its fiduciary duties,

Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach.

COUNT V
Declaratory and Injunctive Relief, 28 U.S.C. § 2201
(On Behalf of Plaintiff and the Nationwide Class)

185. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

186. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

187. Defendant owes a duty of care to Plaintiff and Class Members that required it to adequately secure their PII/PHI.

188. Defendant still possesses Plaintiff's and Class Members' PII/PHI, yet does not adequately protect PII/PHI against the threat of a data breach.

189. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members.

190. Actual harm has arisen in the wake of the Data Breach regarding Defendant's obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII/PHI and Defendant's ongoing failure to address the security failings that led to such

exposure.

191. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the Data Breach.

192. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, being ordered as follows:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

c. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

d. ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

e. ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

f. ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Personal Information not necessary for its provision of services;

g. ordering that Defendant conduct regular database scanning and security checks; and

h. prohibiting Defendant from maintaining PII/PHI of Plaintiff and Class Members on a cloud-based database;

i. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

j. ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive PII/PHI;

k. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding paragraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

l. requiring Defendant to meaningfully educate all class members about the threats they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

m. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the

terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

n. such other and further relief as this Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiff, individually and on behalf of all Class Members, requests judgment against Defendant and that the Court enter an Order:

A. Certifying this action as a class action and appointing Plaintiff and counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

B. Granting equitable relief and enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII/PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. Granting injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

Dated: December 31, 2024

Respectfully submitted,

By: */s/ Andrew W. Ferich*

Andrew W. Ferich*
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com

Counsel for Plaintiff and the Putative Class

** Pro Hac Vice forthcoming*